



EXECUTIVE PERSPECTIVE

LA SOVRANITÀ DIGITALE COME CAPACITÀ STRATEGICA, OPERATIVA E INDUSTRIALE

Dal controllo delle dipendenze
alla costruzione di un modello sostenibile
di innovazione

LA SOVRANITÀ DIGITALE COME CAPACITÀ STRATEGICA, OPERATIVA E INDUSTRIALE

Dal controllo delle dipendenze alla costruzione
di un modello sostenibile di innovazione

INDICE

Prefazione	3
Executive Summary	4
PARTE I — COMPRENDERE LA NUOVA QUESTIONE DELLA SCELTA	
01 Perché la sovranità digitale, e perché adesso	6
PARTE II — LA SOVRANITÀ PRAGMATICA	
02 Oltre la localizzazione del dato	8
03 I livelli di garanzia della sovranità digitale	10
PARTE III — COSTRUIRE LA SOVRANITÀ DIGITALE	
04 Governare la sovranità	14
05 DGS Digital Sovereign Enabler	16
06 AI & Data: l'intelligenza sovrana	20
07 Physical AI: la sovranità del mondo fisico	23
08 Open Source e RIOS: lo stack sovrano	26
09 Cybersecurity: la protezione del perimetro	29
CONCLUSIONI	34

PREFAZIONE

La capacità di scegliere

A cura di Vincenzo Fiengo, Co-CEO di DGS

L'innovazione digitale è stata spesso raccontata come una questione di velocità. Oggi il tema centrale è la libertà di scelta: quali asset deve continuare a governare un'organizzazione per preservare resilienza, capacità decisionale e libertà di evoluzione?

La sovranità digitale nasce da questa domanda. È una sfida industriale, prima ancora che tecnologica: significa mantenere il governo di dati, infrastrutture, piattaforme, competenze, modelli e processi che generano valore e continuità operativa.

L'intelligenza artificiale rende questa sfida ancora più urgente. Serve un approccio pragmatico, capace di distinguere le dipendenze sostenibili da quelle da presidiare e le capacità da preservare nel sistema italiano ed europeo.

DGS è al fianco di imprese e istituzioni con competenze tecnologiche profonde ed esperienza nei contesti critici, contribuendo alla costruzione di regole applicabili e sostenibili per proteggere ciò che è strategico, continuando a innovare.



Vincenzo Fiengo
Co-CEO DGS

SOVRANITÀ DIGITALE

EXECUTIVE SUMMARY

| La sfida **sovrana**

La sovranità digitale è passata dal dibattito geopolitico alle decisioni industriali. La concentrazione dei servizi cloud, la centralità dei dati, la diffusione dell'intelligenza artificiale e l'evoluzione della regolazione europea rendono il controllo delle risorse digitali un fattore di **competitività, resilienza e continuità operativa**.

Alcuni numeri per contestualizzare l'importanza del tema:

85%

del mercato cloud europeo è in mano a tre hyperscaler statunitensi; l'80% della spesa cloud UE va a fornitori USA.

80mld \$

è la spesa mondiale sovereign cloud IaaS nel 2026 (+35,6% sul 2025)

1,8mld €

vale il mercato AI in Italia nel 2025, +50% in un anno; la PA passa dal 6% al 19% (Osservatorio PoliMi)

Il **Cloud and AI Development Act**, proposto dalla Commissione europea il 3 giugno 2026, introduce un quadro unico europeo per valutare la sovranità dei servizi cloud e AI e quattro livelli progressivi di garanzia.

Il modello è destinato in particolare alle valutazioni del rischio e agli acquisti del settore pubblico. La proposta conferma una direzione precisa:

la sovranità deve essere graduata in funzione della criticità e non applicata in modo uniforme.

La localizzazione del dato è solo il primo elemento. Il livello effettivo di sovranità dipende anche dalla giurisdizione applicabile, dal controllo delle identità e delle chiavi, dalla trasparenza della catena software, dalla sostituibilità dei fornitori, dalla disponibilità di competenze e dalla capacità di governare modelli, agenti e decisioni automatizzate.

DGS traduce questa logica in una lettura pragmatica: il settore determina il livello massimo potenzialmente necessario, mentre il singolo workload stabilisce il livello effettivo. La stessa organizzazione può adottare livelli differenti per processi amministrativi, dati regolati, sistemi di controllo e funzioni mission critical.

La risposta non risiede in una singola piattaforma. DGS opera come Digital Sovereign Enabler perché integra la capacità di comprendere dove un'organizzazione si trova e dove deve arrivare con quattro competenze interconnesse: Advisory per definire perimetro, governance, conformità e adozione; AI & Data per governare dati, modelli e agenti; Open Source e RIOS per costruire stack aperti e sostenibili; Cybersecurity per rendere il controllo effettivo e verificabile.

La sovranità digitale coincide con la capacità di scegliere, intervenire, sostituire ed evolvere mantenendo il controllo di ciò che è strategico, senza dover possedere ogni tecnologia.

PARTE I

Comprendere la nuova questione
della scelta

PERCHÉ LA SOVRANITÀ DIGITALE, E PERCHÉ ADESSO

01

Il digitale come infrastruttura **essenziale**

La progressiva digitalizzazione dell'economia ha modificato la funzione della tecnologia nelle organizzazioni. Sistemi applicativi, piattaforme cloud e strumenti di collaborazione non si limitano più a supportare il business: in molti casi coincidono con il processo, ne determinano la continuità e ne condizionano la capacità di evoluzione.

Una **rete energetica** dipende dai **sistemi di monitoraggio** e dispacciamento, un ospedale da ecosistemi di dati e applicazioni, una banca da piattaforme che coordinano **processi, controlli** e **decisioni**.

Questa trasformazione rende le dipendenze tecnologiche una componente del rischio strategico. L'indisponibilità di un servizio, una vulnerabilità della supply chain o un vincolo giuridico sul provider possono produrre impatti che superano il perimetro IT e coinvolgono continuità operativa, reputazione, conformità e capacità decisionale.

| Sicurezza nazionale, **resilienza** e autonomia economica

Sanità, difesa, giustizia, fisco, energia, telecomunicazioni e finanza poggiano su infrastrutture digitali complesse e interconnesse. La resilienza digitale diventa così parte della resilienza economica e istituzionale: proteggere continuità e capacità di ripristino significa tutelare servizi essenziali e ridurre l'esposizione a concentrazioni di mercato, crisi geopolitiche e dipendenze non sostituibili.

La dimensione economica è altrettanto rilevante. Nell'era dell'AI, una quota crescente del valore si concentra nei soggetti che controllano dati, modelli e capacità di calcolo. La sovranità riguarda quindi anche la possibilità di trattenere competenze, proprietà intellettuale e capacità di innovazione, evitando che l'adozione tecnologica coincida con una cessione irreversibile del controllo.

| Le regole europee **trasformano** il mercato

L'Unione europea sta collegando in modo sempre più esplicito competitività, sicurezza e autonomia tecnologica. AI Act, Data Act, Data Governance Act, NIS2, DORA, Cyber Resilience Act e Chips Act intervengono su ambiti diversi, ma convergono su alcuni principi: accountability, portabilità, resilienza, trasparenza della filiera e capacità di verifica.

La proposta di Cloud and AI Development Act rafforza questo orientamento, combinando sviluppo di capacità infrastrutturale, ricerca e innovazione, e un quadro comune europeo per valutare la sovranità dei servizi cloud e AI. Il tema entra quindi nella selezione dei fornitori, nel procurement pubblico e nella progettazione dei servizi destinati ai settori critici.

| Il punto di svolta dell'**intelligenza artificiale**

L'intelligenza artificiale amplia il perimetro del controllo. I sistemi generativi elaborano contenuti e conoscenza; gli agenti richiamano strumenti e interagiscono con applicazioni; la Physical AI collega l'elaborazione digitale a macchine, impianti e infrastrutture. La sovranità non riguarda più soltanto dove risiede il dato, ma anche chi governa il modello, quali strumenti possa usare un agente, quali azioni siano consentite e come sia possibile intervenire.

PARTE II

La sovranità pragmatica

OLTRE LA LOCALIZZAZIONE DEL DATO

02

Perché la **data residency** non basta

La collocazione dei dati nell'Unione europea è un requisito importante, ma non esaurisce la questione. Un dato può essere conservato in un data center europeo e rimanere esposto a una giurisdizione extraeuropea, a procedure operative controllate da soggetti esterni o a piattaforme difficilmente sostituibili. La geografia descrive dove si trova una risorsa; la sovranità descrive chi può esercitare controllo su quella risorsa e a quali condizioni.

Le sei dimensioni del **controllo**

Giuridica

Quale ordinamento si applica a dati, infrastrutture e provider?

Dati

Chi controlla accessi, chiavi, conservazione, lineage e utilizzo?

Operativa

Chi monitora, amministra, ripristina e gestisce le eccezioni?

Tecnologica

Componenti, formati e servizi possono essere sostituiti o migrati?

Industriale

Dove risiedono competenze, proprietà intellettuale e capacità di innovazione?

Cognitiva

Chi governa obiettivi, criteri decisionali, autonomia e supervisione dei sistemi AI?

Considerate insieme, queste dimensioni permettono di distinguere la sola conformità formale dalla capacità concreta di mantenere il controllo sulle dipendenze critiche. La sovranità diventa quindi una proprietà dell'insieme: dati, identità, infrastrutture, software, provider, competenze e processi devono essere letti come una catena unica.

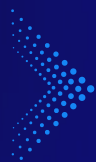
Dalla geografia alla capacità di governo

La domanda manageriale non è se un'organizzazione sia sovrana in senso assoluto.

La domanda è quali funzioni debbano rimanere governabili, quale livello di autonomia richiedano e quali dipendenze possano essere accettate.

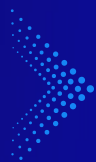
FUNZIONI

Quali devono restare governabili



AUTONOMIA

Quale livello richiedono



DIPENDENZE

Quali si possono accettare

Questa impostazione evita due estremi

CAPACITÀ DI GOVERNO

Dipendenza inconsapevole

Riduce libertà di scelta e resilienza.

Autosufficienza indiscriminata

Aumenta costi e complessità senza produrre necessariamente più valore.

PARTE II

La sovranità pragmatica

I LIVELLI DI GARANZIA DELLA SOVRANITÀ DIGITALE

03

Il quadro proposto dal **Cloud and AI Development Act (CADA)**

La Commissione europea ha adottato il 3 giugno 2026 la proposta di **Cloud and AI Development Act**, orientata a rafforzare l'ecosistema europeo del cloud e dell'intelligenza artificiale. La proposta interviene su tre direttrici: **ricerca e innovazione, sviluppo della capacità infrastrutturale e autonomia**. In quest'ultima area introduce un quadro unico europeo per valutare la sovranità dei servizi cloud e AI, accompagnato da un meccanismo di adozione per il settore pubblico.

Il **CADA** è una proposta di regolamento e potrà essere modificato durante l'iter legislativo.

Il suo impianto rappresenta tuttavia un passaggio rilevante perché definisce quattro livelli progressivi di garanzia, da utilizzare sulla base della valutazione del rischio.

La classificazione non coincide con la precedente tassonomia editoriale del deck DGS e richiede quindi una formulazione aderente al quadro ufficiale.



I 4 livelli del CADA

Livello 1

LOCALIZZAZIONE EUROPEA DEI DATI

Adatto per processi di business non critici o di supporto ordinario (es. portali informativi, elaborazioni non sensibili), dove il rischio principale è mitigato dalla semplice localizzazione ed elaborazione dei dati all'interno dei confini UE

Livello 2

INDIPENDENZA OPERATIVA E TRASPARENZA DELLA SUPPLY CHAIN

Necessario per processi a media/alta criticità, dove un'interruzione o il blocco dei servizi da parte del fornitore cloud/AI creerebbe danni operativi significativi. Richiede autonomia di gestione e trasparenza sui subfornitori.

Livello 3

PROPRIETÀ E CONTROLLO EUROPEI

Indicato per processi core/strategici (es. settori regolati, servizi finanziari, sanità, infrastrutture critiche NIS2), in cui la continuità operativa e la riservatezza non possono dipendere da soggetti controllati da Paesi terzi.

Livello 4

PIENA SOVRANITÀ E CONTROLLO SULLA SUPPLY CHAIN SOFTWARE

Riservato ai processi con massimo grado di criticità e sicurezza nazionale (es. difesa, intelligence, funzioni giudiziarie essenziali), dove il rischio di ingerenza esterna deve essere azzerato a livello di codice, infrastruttura e manutenzione.

Il quadro europeo supera quindi l'equivalenza tra localizzazione e sovranità. Al crescere del livello aumentano i requisiti relativi a indipendenza da Paesi terzi, proprietà e controllo, trasparenza e governo della catena software.

Il contributo DGS: applicare i livelli ai workload

I livelli europei definiti dal CADA qualificano le caratteristiche del servizio e del provider. Il contributo DGS consiste nel tradurli nel contesto concreto dell'organizzazione, partendo dalla criticità del settore, dalla sensibilità dei dati, dall'impatto dell'interruzione, dagli obblighi normativi e dalla sostituibilità delle componenti.

Il settore stabilisce il tetto. Il singolo workload determina il livello effettivamente necessario sotto quel tetto.

Una stessa organizzazione può legittimamente adottare livelli differenti. Un portale amministrativo e un ambiente di sviluppo possono richiedere garanzie inferiori rispetto a un sistema di controllo, a una piattaforma finanziaria critica o a un'infrastruttura preposta alla gestione di dati classificati. La sovranità pragmatica concentra le misure più stringenti dove il valore e il rischio lo richiedono, preservando sostenibilità economica e accesso all'innovazione negli altri ambiti.

CONTESTO

ORIENTAMENTO DI MASSIMA

ENTERPRISE
GENERIC



Livelli di base per i workload ordinari; innalzamento selettivo per dati sensibili o processi critici.

INDUSTRIE
REGOLATE



Livelli differenziati in funzione di proprietà intellettuale, requisiti cyber e casi d'uso ad alto rischio.

FINANZA E
ASSICURAZIONI



Garanzie elevate per dati regolati, processi decisionali e servizi essenziali.

INFRASTRUTTURE
CRITICHE



Livelli superiori per sistemi di controllo e dispacciamento; approcci differenziati per le funzioni amministrative.

DIFESA E
SICUREZZA NAZIONALE



Massimo livello di garanzia per infrastrutture classificate, intelligence e dati coperti da segreto.

I fattori chiave da considerare nella valutazione

01

Natura e sensibilità dei dati trattati

ad esempio dati personali, finanziari, sanitari o legati a informazioni industriali strategiche.

02

Criticità del servizio per la continuità operativa

ovvero la distinzione tra processi core, il cui blocco comprometterebbe l'operatività aziendale, e processi di supporto o back-office, meno critici.

03

Dipendenza tecnologica e di governance

in particolare l'esposizione a normative extra-UE, come ad esempio il CLOUD Act statunitense, che possono incidere sul controllo reale dei dati.

04

Rilevanza per l'ordine pubblico e la sicurezza delle infrastrutture critiche

aspetto che assume particolare rilevanza per gli enti pubblici e per i soggetti rientranti nel perimetro della direttiva NIS2.

PARTE III

Costruire la sovranità digitale

GOVERNARE LA SOVRANITÀ

D4

Dalla classificazione al programma

La classificazione stabilisce il livello di garanzia necessario; la governance trasforma quella scelta in un programma attuabile. La sovranità richiede decisioni su architetture, fornitori, contratti, responsabilità, controllo operativo, competenze e investimenti. La tecnologia è essenziale, ma non sufficiente:

un ambiente può
possedere
caratteristiche sovrane e
rimanere non
governabile se mancano
ruoli, processi e capacità
di verifica.



| Perimetro, governance, conformità e adozione

01 | PERIMETRO

OBIETTIVO

Classificare dati, processi, sistemi e fornitori per criticità, rischio e dipendenza.

02 | GOVERNANCE

OBIETTIVO

Definire responsabilità, modello operativo, metriche e meccanismi decisionali.

03 | CONFORMITÀ

OBIETTIVO

Tradurre AI Act, NIS2, DORA, GDPR, Data Act e CADA in requisiti verificabili.

04 | ADOZIONE

OBIETTIVO

Sviluppare competenze, processi e cultura necessari a governare ciò che è stato scelto.

La sovranità è sostenibile quando entra nei processi ordinari di sourcing, sviluppo, sicurezza, gestione e cambiamento. Il go-live non è il traguardo: dipendenze, normative e tecnologie evolvono, e il modello deve essere aggiornato attraverso monitoraggio, riesame del rischio, test di portabilità e verifica della continuità.

PARTE III

Costruire la sovranità digitale

DGS DIGITAL SOVEREIGN ENABLER

05

Conoscere il punto di partenza e definire la destinazione

DGS accompagna le organizzazioni nella lettura del proprio contesto, nella valutazione del punto di partenza rispetto ai requisiti di sovranità e nella definizione del percorso per raggiungere il livello necessario. Questa capacità precede la scelta tecnologica:

occorre comprendere ciò che deve essere **protetto**, distinguere le **dipendenze accettabili** da quelle critiche e **collegare ogni decisione a rischio, conformità e obiettivi di business**.

L'Advisory svolge quindi una funzione trasversale: trasforma criteri normativi e esigenze di controllo in **perimetro, roadmap, modello operativo e programma di adozione**. DGS classifica dati, processi e sistemi, misura la dipendenza dai fornitori, individua il livello di garanzia adeguato e definisce priorità, investimenti, responsabilità e metriche.

DGS Sovereign Enabler: competenze interconnesse

La sovranità digitale è il risultato di un percorso integrato che combina piattaforme, infrastrutture, certificazioni e competenze. DGS la rende concreta attraverso la convergenza di quattro aree di competenza che presidia e mette a fattor comune: **Advisory, AI & Data, Open Source** e **Cybersecurity**.

ADVISORY

Perimetro e governance

Strategia, modello operativo e governance della sovranità digitale, tradotti in roadmap, processi, ruoli e metriche misurabili.

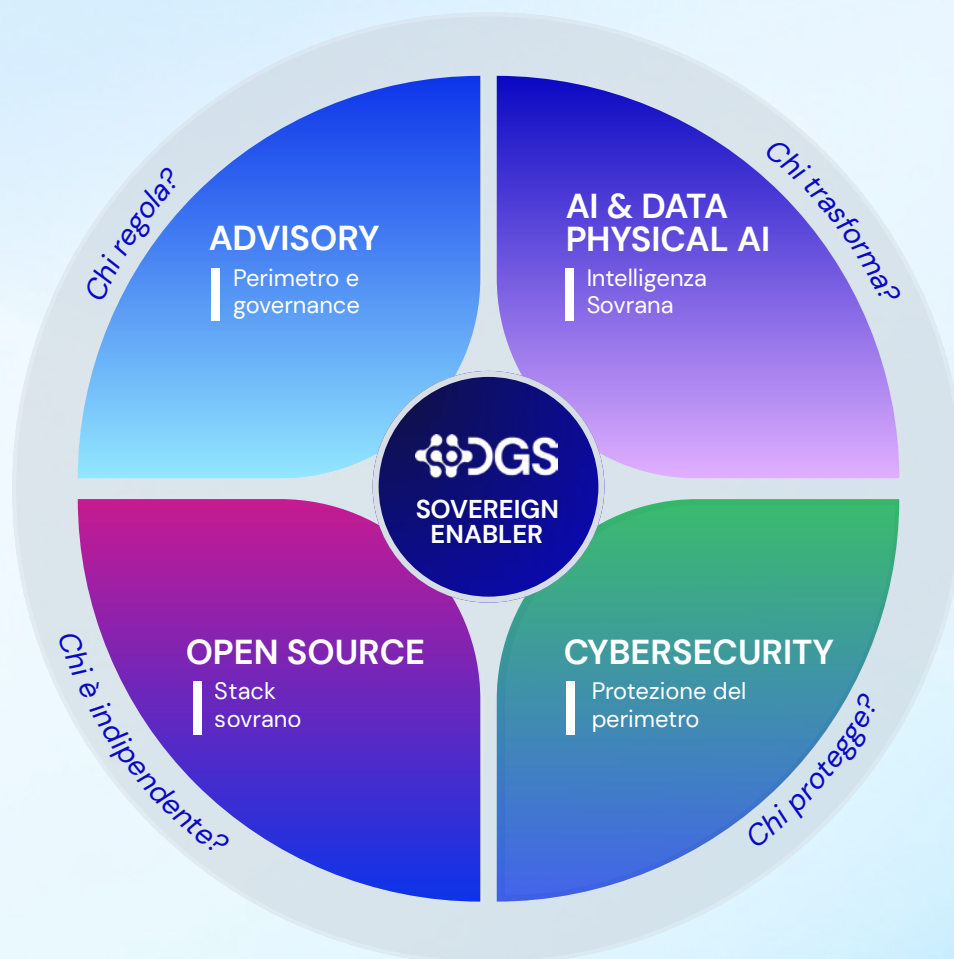
- SCOPE
- COMPLIANCE
- GOVERNANCE
- ADOPTION

AI & DATA SENSE | PHYSICAL AI

Intelligenza sovrana

Piattaforme dati e soluzioni di AI: dai modelli agli agenti, fino all'AI fisica. Ogni agente ha identità, responsabile e traccia verificabile.

- AI & DATA SOLUTIONS
- DATA MARKETING
- AGENTIC ORCHESTRATION
- AI ENGINEERING



OPEN SOURCE

Stack sovrano

Infrastrutture su tecnologie aperte: trasparenza, portabilità, indipendenza dai fornitori. Siamo protagonisti di RIOS: non utilizzatori, ma costruttori.

- RIOS (RETE ITALIANA OPEN SOURCE)
- VERTICAL AI & DATA
- ENTERPRISE SOLUTIONS

CYBERSECURITY

Protezione del perimetro

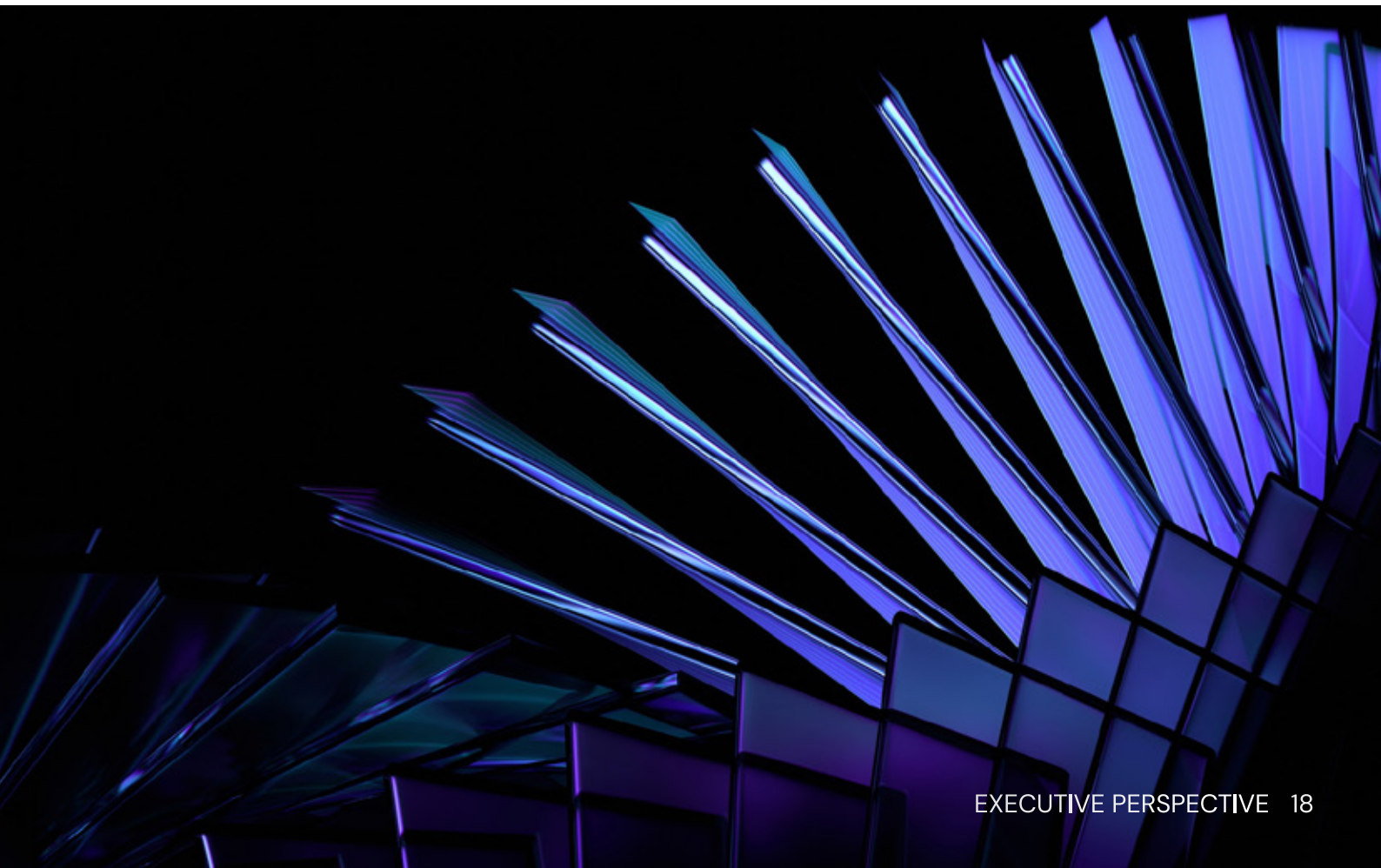
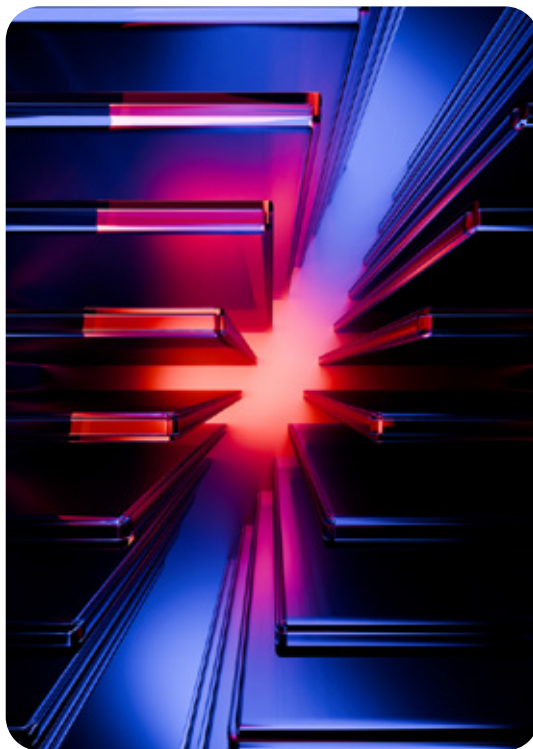
Protezione di dati, identità e servizi con Governance & Compliance, monitoraggio, gestione del rischio e controllo degli accessi, per integrità e resilienza.

- AI SECURITY
- CUSTOMIZED SOLUTIONS
- MANAGED SECURITY SERVICES

Comporre, integrare, costruire

Il ruolo di DGS è quello di un **orchestratore sovrano**, ovvero di comporre l'architettura più adeguata attraverso ambienti dedicati, tecnologie aperte e capacità di calcolo disponibili, senza replicare l'infrastruttura dei grandi provider né vincolare il cliente a un unico stack.

La **sovranità** diventa così una **proprietà dell'architettura** e del modello operativo, non l'etichetta di un singolo prodotto.



| Dove DGS costruisce **valore** nella catena sovrana

La catena della sovranità digitale comprende strati molto differenti. Silicio, energia, data center e capacità di calcolo richiedono investimenti infrastrutturali e sono presidiati dai grandi operatori globali. DGS concentra il proprio valore sugli strati in cui contano selezione, composizione, integrazione e governo del rischio, componendo le diverse capacità disponibili in funzione del costo e del grado di controllo richiesto.

Il valore si concentra negli strati in cui contano conoscenza del dominio, fiducia, integrazione e capacità di gestione: piattaforma e orchestrazione, applicazioni verticali, governance, conformità e adozione. È qui che requisiti generali diventano soluzioni coerenti con i processi reali di PA, difesa, finanza, energia, sanità e industrie regolamentate.

STRATO

Governance, conformità e adozione

RUOLO DGS

Tradurre norme e obiettivi di autonomia in programmi, controlli, ruoli e competenze.

STRATO

Applicazioni verticali sovrane

RUOLO DGS

Integrare la sovranità nei processi specifici di settore e nei sistemi core.

STRATO

Piattaforma e orchestrazione

RUOLO DGS

Coordinare dati, modelli, agenti, identità, audit e workload tra ambienti differenti.

STRATO

Cloud e capacità di calcolo

RUOLO DGS

Selezionare e comporre provider europei, ambienti dedicati e servizi globali governati.

Avere un partner capace di trasformare requisiti complessi in scelte concrete: quali componenti utilizzare, quali dipendenze accettare, quali controlli introdurre e come mantenere il governo del sistema nel tempo.

In questo ruolo, DGS integra competenze tecniche, conoscenza dei processi, capacità di delivery e relazioni di ecosistema, così da rendere l'architettura coerente con il livello di rischio, gli obiettivi dell'organizzazione e le condizioni reali di esercizio.

PARTE III

Costruire la sovranità digitale

AI & DATA: L'INTELLIGENZA SOVRANA

06

Dati, modelli e agenti lungo tutto lo stack

Per DGS, la sovranità dell'intelligenza coincide con la capacità di governare l'intero sistema che trasforma dati, modelli e agenti in risultati operativi. Il perimetro attraversa business layer, applicazioni, dati, software e infrastruttura; comprende strategia e adozione, sviluppo di casi d'uso, data governance, AI Engineering, messa in esercizio e sicurezza.

Il dato costituisce il fondamento. Qualità, tracciabilità, lineage, criteri di accesso e condizioni di utilizzo devono essere governati lungo il ciclo di vita.

Un modello affidabile richiede dati affidabili e un'organizzazione in grado di sapere da dove provengono, come sono stati trasformati e con quali vincoli possono essere utilizzati.

Orchestrare modelli e piattaforme

Modelli proprietari, modelli aperti, ambienti cloud e infrastrutture dedicate offrono vantaggi e vincoli differenti. DGS governa queste dipendenze attraverso un approccio di orchestrazione: selezionare la componente più adatta al caso d'uso, integrarla con i sistemi del cliente e mantenere la possibilità di sostituirla o modificarla quando cambiano rischio, prestazioni o requisiti.

AI Factory, strumenti di AI Engineering e ambienti MLOps/LLMOps rendono industriale questo processo. Modelli, dati, valutazioni, controlli e requisiti di sicurezza vengono ricondotti a una catena governabile e ripetibile, nella quale la velocità di sperimentazione non compromette qualità, tracciabilità e controllo.



Selezionare

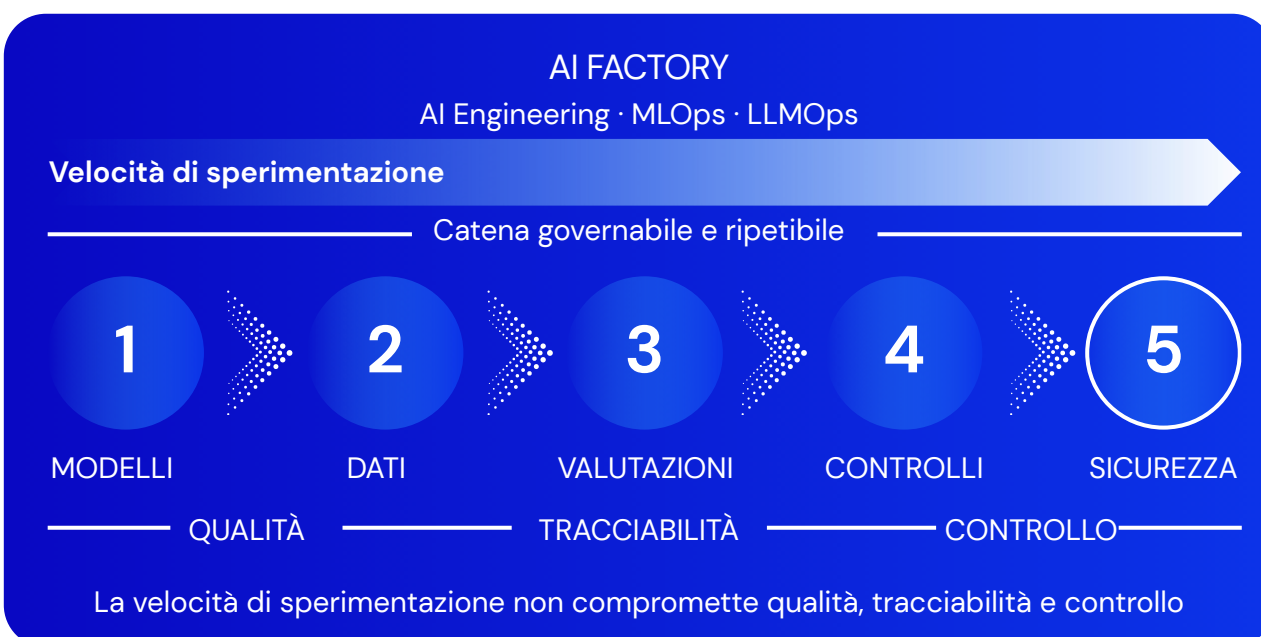
la componente più adatta al caso d'uso

Integrare

con i sistemi del cliente

Sostituire

o modificare, quando cambiano rischio, prestazioni o requisiti



Governare il paradigma agentico

Gli agenti segnano il passaggio da sistemi che producono risposte a sistemi che eseguono attività. La sovranità si sposta dal risultato all'azione: identità, autorizzazioni, strumenti, memoria, interazioni e livelli di autonomia devono essere definiti e monitorati. Ogni agente deve essere riconoscibile, associato a un perimetro operativo e inserito in una catena di responsabilità verificabile.

DGS integra orchestrazione agentica, data governance, sicurezza e gestione applicativa affinché supervisione, tracciabilità e possibilità di intervento siano parte dell'architettura. L'obiettivo è **ampliare l'adozione dell'AI** senza separare autonomia operativa e accountability.

PARTE III

Costruire la sovranità digitale

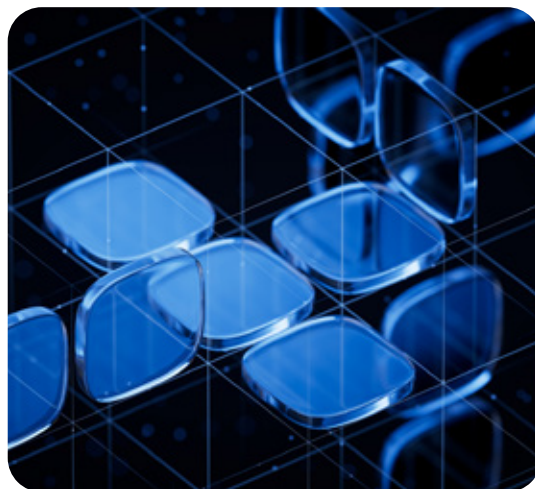
PHYSICAL AI: LA SOVRANITÀ DEL MONDO FISICO

07

Quando il controllo riguarda il comportamento

La Physical AI porta l'intelligenza artificiale oltre lo schermo. Robot mobili, sistemi autonomi, digital twin, computer vision, edge AI e piattaforme OT collegano informazione e azione.

In questo scenario, **la sovranità non riguarda soltanto chi controlla il dato**, ma chi determina il comportamento del sistema, con quali garanzie e attraverso quale filiera.



Quattro dimensioni della Physical AI sovrana

01 | DATI

PRESIDIO

Il dato nasce sul campo: edge inference, OT data governance e conservazione nel perimetro.

02 | MODELLI

PRESIDIO

Simulazione, digital twin e ambienti sim-to-real controllabili e ispezionabili.

03 | AZIONE

PRESIDIO

Identità dell'agente, autorizzazione dei comandi critici, traccia verificabile e fermo sicuro.

04 | FILIERA

PRESIDIO

Hardware, firmware, sensori, SBOM, portabilità e criteri di supply chain.

Trieste: un ecosistema per la sperimentazione sim-to-real

DGS punta a creare ambienti controllati, fisici e digitali, nei quali digital twin, agenti e sistemi robotici possano essere addestrati, collaudati e verificati attraverso simulazioni sim-to-real prima dell'impiego nei processi reali.

Un percorso da costruire insieme all'ecosistema scientifico e industriale del territorio, per tradurre la Physical AI in applicazioni sicure, verificabili e coerenti con i requisiti di sovranità.

Trieste rappresenta il **contesto naturale** in cui sviluppare questa visione, grazie alla **convergenza tra ricerca scientifica, porto, logistica, cantieristica e osservazione marittima.**

Nel disegno strategico al 2028, l'ambizione è evolvere progressivamente verso quella che potrebbe diventare la "prima palestra sovrana europea" per la Physical AI: un ambiente nel quale dati, modelli, telemetria e proprietà intellettuale restino all'interno di un perimetro governato, con sicurezza OT, tracciabilità e supervisione integrate fin dalla progettazione.



PARTE III

Costruire la sovranità digitale

OPEN SOURCE E RIOS: LO STACK SOVRANO

08

Dall'apertura tecnologica alla capacità industriale

L'Open Source è una leva di sovranità perché favorisce trasparenza, standard aperti, interoperabilità, portabilità e libertà di evoluzione. L'accesso al codice, tuttavia, non produce automaticamente autonomia: senza governance, competenze, manutenzione, sicurezza e supporto enterprise, una piattaforma aperta può generare una nuova dipendenza.

Per DGS, fare Open Source significa mantenere e contribuire al software, presidiare la sicurezza della supply chain, garantire supporto e continuità, partecipare ai riferimenti istituzionali e anticipare gli orientamenti europei.

Lo **stack sovrano** attraversa infrastrutture, piattaforme abilitanti e soluzioni verticali, sostenute trasversalmente da **governance** e **supporto**, e da un **ecosistema capace di farle evolvere**.

DGS e RIOS: non utilizzatori, ma costruttori dell'ecosistema

RIOS, la **Rete Italiana Open Source**, di cui DGS è co-founder, membro di **APELL** (The European Open Source Software Business Association), offre alle organizzazioni un ecosistema di competenze e tecnologie capace di rendere l'Open Source una scelta sostenibile anche in contesti complessi. La rete mette in relazione aziende italiane specializzate e una capacità distribuita fatta di:

- oltre 400 technical specialists**

- 27 partner ufficiali tra vendor e community**

- 80 certificazioni tecniche**

- formatori dedicati**

- un ampio patrimonio di prodotti, framework e tecnologie**

Per il cliente, questo significa poter contare su capacità distribuite di sviluppo, integrazione, formazione e supporto, riducendo il rischio che l'adozione di tecnologie aperte si traduca in una nuova dipendenza operativa.

Il valore di RIOS va oltre il catalogo tecnologico. Una dipendenza digitale è spesso anche una dipendenza di competenze: accedere al codice non basta se mancano persone in grado di comprenderlo, adattarlo, proteggerlo e mantenerlo. RIOS riduce questa distanza unendo specializzazioni complementari e rendendo disponibile un ecosistema in grado di sostenere architetture e programmi complessi.

Dalla capacità nazionale alla dimensione europea

La partecipazione di RIOS ad APELL collega le competenze italiane al confronto europeo sull'Open Source. Questo presidio permette di contribuire agli orientamenti istituzionali, partecipare all'evoluzione degli standard e rappresentare le esigenze delle imprese che sviluppano e adottano tecnologie aperte. La sovranità non si costruisce in isolamento: richiede capacità nazionali inserite in reti europee.

Molte aziende utilizzano **Open Source**.
DGS, attraverso **RIOS**, contribuisce a costruire l'ecosistema che lo rende una leva concreta di sovranità tecnologica e industriale.

Quattro dimensioni per rendere l'Open Source governabile

01 Sovranità tecnologica

ARCHITETTURE APERTE,
INTEROPERABILI E VERIFICABILI

02 Sovranità delle competenze

SPECIALISTI, CERTIFICAZIONI,
FORMAZIONE E SUPPORTO.

03 Sovranità industriale

CAPACITÀ DI SVILUPPARE, MANTENERE E
FAR EVOLVERE SOLUZIONI NEL TEMPO

04 Sovranità di ecosistema

COLLEGAMENTO TRA ECCELLENZE ITALIANE,
COMMUNITY E RAPPRESENTANZA EUROPEA

PARTE III

Costruire la sovranità digitale

CYBERSECURITY: LA PROTEZIONE DEL PERIMETRO

09

Rendere il controllo continuo e verificabile

La **cybersecurity** è il presidio che rende la sovranità digitale effettiva nel tempo. Dati localizzati, infrastrutture dedicate, tecnologie aperte e modelli di AI governati producono valore solo se l'organizzazione mantiene il controllo su identità, accessi, vulnerabilità, componenti software, superfici esposte e minacce.

Questo significa poter sapere chi accede a cosa, con quali privilegi, da quali ambienti, attraverso quali tecnologie e con quali evidenze.

La sicurezza diventa una condizione di governo: consente di ridurre l'esposizione, rendere verificabili le scelte architettureali e mantenere il livello di garanzia definito anche quando cambiano rischio, normativa o tecnologia.

AMBITO

Dati e identità

BENEFICI PER IL CLIENTE

Controllare accessi, privilegi, chiavi, tracciabilità e responsabilità sulle risorse critiche.

AMBITO

Tecnologia e supply chain

BENEFICI PER IL CLIENTE

Rendere verificabili componenti, piattaforme, dipendenze software e superfici esposte.

AMBITO

Conformità

BENEFICI PER IL CLIENTE

Tradurre NIS2, DORA, CRA, AI Act e GDPR in controlli, evidenze e auditabilità.

AMBITO

Resilienza

BENEFICI PER IL CLIENTE

Rilevare, contenere, ripristinare e mantenere operative le funzioni essenziali.

| **AI Security: proteggere modelli, agenti e azioni**

L'intelligenza artificiale estende il perimetro della sicurezza a dati, applicazioni, modelli, agenti, strumenti, prompt, memoria, autorizzazioni e azioni automatizzate. Un sistema AI può accedere a informazioni sensibili, richiamare tool, generare output e attivare processi: ogni passaggio deve essere governato.

Nel concreto, AI Security significa adottare l'AI mantenendo responsabilità, supervisione e capacità di intervento. Ogni agente deve avere un'identità, un perimetro operativo, privilegi proporzionati e una traccia verificabile. Prompt injection, abuso degli strumenti, compromissione degli agenti, alterazione dei modelli e escalation dei privilegi diventano rischi da gestire con controlli tecnici, processi e monitoraggio continuo.

| **Resilienza e continuità operativa**

La sovranità digitale si misura anche nella capacità di reggere una crisi. Un'organizzazione deve poter rilevare rapidamente un incidente, contenerne gli effetti, preservare le funzioni essenziali e ripristinare servizi e dati. Questo presidio riguarda gli ambienti IT, ma anche quelli OT e IoT, dove un incidente può estendersi a impianti, infrastrutture, servizi essenziali e processi fisici.



In questa prospettiva, **SOC, servizi gestiti, incident response, threat intelligence, identity security, OT security e continuità operativa** non sono componenti separate, ma parti di una stessa capacità: mantenere il controllo anche quando l'ecosistema è sotto pressione.

Dal modello ai percorsi di trasformazione

Il contributo DGS consiste nel collegare assessment, progettazione, realizzazione e gestione continua. Il punto di partenza è la mappatura di asset, dipendenze, rischi, esposizioni e requisiti; il passo successivo è la costruzione di ambienti, piattaforme, controlli e processi coerenti con il livello di garanzia richiesto; la fase di esercizio mantiene nel tempo evidenze, resilienza e conformità.

FASE

VALUTARE ESPOSIZIONE E DIPENDENZE

COSA CONSENTE AL CLIENTE

Mappare asset, identità, superfici esposte, fornitori critici, componenti software e requisiti normativi per capire dove il controllo è più fragile.

FASE

DISEGNARE CONTROLLI E RESPONSABILITÀ

COSA CONSENTE AL CLIENTE

Definire ruoli, privilegi, policy, approvazioni, requisiti di audit e criteri di sicurezza coerenti con il livello di garanzia richiesto.

FASE

PROTEGGERE DATI, IDENTITÀ E AMBIENTI

COSA CONSENTE AL CLIENTE

Applicare controlli su accessi, chiavi, privilegi, workload, componenti applicative e infrastrutture IT, cloud, OT e AI.

FASE

MONITORARE E REAGIRE

COSA CONSENTE AL CLIENTE

Rilevare anomalie, minacce e incidenti con presidio continuativo, capacità di risposta e tracciabilità delle evidenze.

FASE

MANTENERE RESILIENZA E CONFORMITÀ

COSA CONSENTE AL CLIENTE

Aggiornare controlli, verifiche, metriche e piani di continuità per preservare nel tempo sicurezza, auditabilità e capacità di ripristino.

Questi ambiti vengono combinati in funzione del contesto, della maturità del cliente e della criticità dei workload. La continuità tra strategia, progetto e gestione è ciò che distingue una dichiarazione di sovranità da una capacità realmente esercitabile:

la sicurezza rende visibile ciò che **accade**,
verificabile ciò che è stato deciso e **governabile**
ciò che deve restare sotto controllo.

CONCLUSIONI

La sovranità come capacità da esercitare

La sovranità digitale è la capacità di scegliere, intervenire, sostituire ed evolvere mantenendo il controllo di ciò che è strategico. Non coincide con la sola localizzazione del dato né con una piattaforma, ma con un modello proporzionato alla criticità dei workload e verificabile nel tempo.

Il contributo di DGS

DGS traduce questa logica in percorsi concreti: il settore definisce il livello massimo potenzialmente necessario, il singolo workload determina il livello effettivo di garanzia.

Da questa lettura derivano scelte su **architetture, fornitori, dati, modelli, agenti, sicurezza e continuità operativa**.

| Esperienza nei contesti critici

PA, difesa, finanza, energia e industrie regolamentate sono ambiti in cui controllo, sicurezza e conformità sono esigenze operative.

Traduzione dei requisiti in scelte concrete

Il percorso permette di definire dati, sistemi, processi e dipendenze che richiedono maggiore presidio.

Competenze integrate

Advisory, AI & Data, Open Source, RIOS e Cybersecurity vengono combinati in un percorso unico, dalla valutazione iniziale alla gestione continuativa.

Radicamento italiano e dimensione europea

La prossimità al contesto nazionale si integra con ecosistemi come RIOS e APELL, rafforzando competenze, supporto e capacità di evoluzione.

Approccio proporzionato

Ogni percorso viene costruito sulla base del rischio, della maturità dell'organizzazione e degli obiettivi di business.

La **sovranità** non è possedere ogni cosa. È **poter scegliere**, sempre, da chi dipendere e a quali condizioni. **DGS** esiste per rendere questa **scelta possibile, sicura e italiana**.

HANNO CONTRIBUITO

Antonio Autorino

Head of AI & Data Sense

Michele Balbi

Advisor Digital Innovation Strategy

Giuseppe Blasi

Partner, Management Consulting

Pierluigi Brienza

Chief Strategy Officer

Gianluca Cimino

Chief Strategy & Delivery Officer Cybersecurity

Biagio De Marchis

Chief Business Growth Officer

Francesco Di Bianco

Physical AI Offering Leader

Irene Cosimo

Content Marketing Leader

Milena Fabbrizzi

AI & Data Business Developer

Alessandro Favretto

AI – Service Line Manager

Eraldo Federici

Chief Operating Officer Digital Solutions

Roberta Giani

Chief Marketing & Communication Officer

Fabio Storri

Head of Consulting Strategic Offering

Marco Tessarin

Head of Open Source Excellence Center

| Chi è DGS

DGS S.p.A. è il partner tecnologico italiano che da 29 anni affianca la crescita di imprese e pubbliche amministrazioni attraverso la modernizzazione in sicurezza di processi, sistemi e infrastrutture, grazie a una conoscenza approfondita delle tecnologie e dei mercati.

Con un'offerta che integra servizi di Cybersecurity, AI & Data, Digital Engineering, Management Consulting e soluzioni per la Smart Enterprise, DGS accompagna le organizzazioni nella costruzione di basi solide e fiducia digitale per il miglioramento delle performance operative, della resilienza e della sostenibilità dei processi, attraverso percorsi di AI modernization e un approccio Secure by Design.

DGS opera attraverso un modello di Centri di Eccellenza e di partnership con i principali vendor tecnologici globali. Il Gruppo conta oltre 2.700 professionisti e più di 2.500 certificazioni tecniche.

Proprietà intellettuale e riservatezza del documento

Proprietà Intellettuale

Tutti i contenuti, le informazioni, le metodologie, i modelli, il software, gli elaborati, le rappresentazioni grafiche e la documentazione descritti nel presente materiale sono di esclusiva titolarità di DGS S.p.A., salvo diversa indicazione espressa.

La riproduzione, distribuzione, pubblicazione, modifica o utilizzo, anche parziale, dei contenuti è vietata senza il preventivo consenso scritto di DGS S.p.A.

Riservatezza

Il presente documento contiene informazioni riservate e proprietarie di DGS S.p.A. ed è destinato esclusivamente alle finalità connesse alla valutazione della candidatura.

È vietata la divulgazione, distribuzione o comunicazione a terzi dei contenuti qui riportati senza il preventivo consenso scritto di DGS S.p.A., fatti salvi gli utilizzi strettamente necessari alle attività di valutazione da parte degli organizzatori dell'iniziativa.

Le informazioni contenute nel presente documento sono fornite esclusivamente a fini illustrativi e non comportano alcuna concessione, licenza o trasferimento di diritti di proprietà intellettuale, industriale o di know-how in favore di terzi."

CONTATTACI

 @dgs_spa

 DGS SpA

 www.dgsspa.com



visit dgsspa.com